KDDI Europe

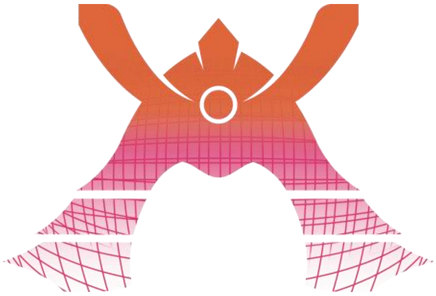
Threat Report

Volume 3

July 2025

Table Of Contents

Introduction



Welcome to the Threat Report. The purpose of this document is to provide an overview of the latest cybersecurity threats and trends that could impact organisations worldwide. By analysing recent incidents and emerging threats, we aim to equip our team and customers with the knowledge and insights necessary to proactively defend against potential attacks.

At KDDI Europe, our dedication to protecting our clients and their systems is unwavering. We are continuously investing in security technologies and training our staff to enhance defences and respond swiftly to any threats. We are deeply committed to ensuring that our customers are protected in accordance with the highest standards of cybersecurity.

It is our belief that our success is linked to the success of our customers' businesses. By safeguarding your operations, we aim to provide a secure environment where your business can thrive and grow. Thank you for taking the time to review this report.

NEWS

The Latest Cybersecurity News

United Natural Foods, Inc suffers cyber attack[1]

One of the largest publicly traded wholesale distributors of health and speciality food in the United States of America has suffered a cyberattack. Not much is known about the incident at this stage, but a regulatory filing was made on Monday 9th June to confirm the attack. . The company said it become aware of the attack on the 5th of June 2025 after they noticed unauthorised activity in their systems, as a result, they took some systems offline to mitigate the attack while they continue to investigate.

Bitdefender aims to Expand Email Security Capabilities through acquisition[2]

Bitdefender, a major cybersecurity vendor announced on the 18th of June 2025 that it has agreed to acquire Mesh Security Limited also known as Mesh. Mesh is an email security platform built for MSPs and the integration of their technologies with Bitdefender's Extended Detection and Response (XDR) and MDR services is intended to boost the email security capabilities of Bitdefender.

The acquisition is subject to regulatory approvals and customary closing conditions however the terms of the transaction have not yet been disclosed.

Insights

Email Security

Email remains a significant vector for cyberattacks and one thing is evident, people are always going to click on links, buttons and anything else that causes the mouse cursor to change from its default triangular pointer to one which indicates that an item is clickable.

Email security solutions are able to filter incoming emails and accurately detect spam, but every now and then a fraudulent email makes its way into the inbox of an unsuspecting employee, what happens then?

Attackers are smart, they know to send emails when fatigue has set in after a long day of work and employees are exhausted. Or at the end of a month when a business would be expecting invoices or correspondence from suppliers, partners etc. So, by sending emails when they are likely to be expected or when the individual is most prone to not paying attention, then adding the apparent compulsion everyone has to click everything on the screen, threat actors increase the likelihood of having their malicious links clicked. ? If someone as experienced as Troy Hunt, a Microsoft Regional Director, web security consultant, and the creator of “Have I Been Pwned” can fall for a phishing attack due to fatigue, then it can happen to anyone.

Is it possible to stay on guard all the time? Possibly, but when you consider the amount of damage a single email can cause it becomes clear that vigilance is not just a best practice, it’s a necessity. While no system or individual can maintain perfect awareness at all times, organisations must invest in layered security strategies that combine advanced email filtering, continuous user education, and real-time threat detection.

Ultimately, fostering a culture of cybersecurity awareness where employees are empowered to pause, question, and verify can be the most effective defence against the ever-evolving tactics of cybercriminals.

Suggestions

Protection, Prevention and Takeaways

1

Consider scheduled reviews of user access and permissions. Businesses need to consider who has access to what and how long they need access for. Especially for accounts that are not created on Entra ID or the Active Directory. After users leave organisations, change departments or simply no longer require access then these accounts should be properly handled. If such an account were to be compromised, then it would take a while before anyone noticed would it not?

2

Since email is still one of the most prevalent vectors of attack then no organisation that can afford it should be without some form of email protection. It is not enough to have security awareness training for staff, the organisation must support the users' efforts as well. Having spam filters, anti-phishing tools, and malware detection to protect against email-based threats should be the least measure that a business puts in place. Combining user education with technical defences creates a layered security approach, which is more effective in mitigating risks.

3

There is no explicit legal requirement that mandates an organisation to inform its customers if a similar domain name is being used by scammers to impersonate their brand, however for the purposes of reputation management and customer protection this should be done where possible. There are Open Source Intelligence tools available that can easily provide information about domain names that bear similarity to your business' domain. It would be prudent to take a look and see who may be attempting to scam your customers so you can act.

Common Vulnerabilities and Exposures (CVE)

Every month a CVE is selected at the discretion of the reports author discussed. This report will now also include the EUVD ID as well. This month it is a vulnerability affecting one of the most popular web browsers in the world.

CVE-2025-5419 | EUVD-2025-16695

Vendor : Google

Product : Chrome

Published : 02 July 2025

Platform : Windows, macOS and Linux

Description

It is a high-severity vulnerability in Google Chrome's V8 JavaScript engine that allows remote attackers to exploit heap corruption through a crafted HTML page.

What does this mean for you?

If a user accesses an HTML page crafted by a remote attacker that exploits CVE-2025-5419, it could lead to several serious consequences, including remote code execution, data theft, malware installation and browser compromise.

What should you do about it?

Update Chrome to 137.0.7151.68/.69 or a higher version for Windows, Mac and 137.0.7151.68 or higher version for Linux.

Links & References

1. https://edition.cnn.com/2025/06/09/food/united-natural-foods-cyberattack
2. https://www.bitdefender.com/en-us/news/bitdefender-to-acquire-mesh-security-expanding-its-email-security-capabilities
3. https://www.cvedetails.com/cve/CVE-2025-5419/

Contact Us

KDDI Europe is a growing ICT solution provider based in London and a subsidiary of KDDI Corporation. It is the regional headquarters of EMEA and CIS regions offering a host of ICT services as a 'One-Stop' solution, including cloud computing, data centre, IT consulting, IT outsourcing, network, security, system integration and voice services.

The excellent reputation and trust enjoyed by our Telehouse data centres positioned around the world have kept us at the forefront of service and quality

Contact Information

Telephone Number	+44 20 7507 0001
Email Address	info@uk.kddi.eu
LinkedIn	https://linkedin.com/company/kddi-europe-limited

Website

LinkedIn